Claims

We claim:

1. A data carrier comprising:

an identification number associated with the data carrier;

a memory for storing a one-time pad and data, wherein the one-time pad is uniquely associated with the identification number;

an encryption circuit, coupled to the memory, for encrypting the data with the one-time pad; and

a controller, coupled to the memory, to prevent reuse of bits in the one-time pad.

2. The data carrier of claim 1 wherein the encryption circuit performs an exclusive-or function.

3. The data carrier of claim 1 further comprising a counter, coupled to the memory, to index to a next bit in the one-time pad.

4. The data carrier of claim 1 further comprising an interface, wherein the interface comprises at least one of the following: capacitive coupling, inductive coupling, electromagnetic coupling, optical coupling, electrical coupling, and contact.

5. The data carrier of claim 1 further comprising a power supply that receives energy from a reader via at least one of capacitive coupling, inductive coupling, electromagnetic coupling, optical coupling, and contact.

6. The data carrier of claim 1 further comprising a power supply that receives energy from on of the following: a battery, and a super-capacitor.

7. The data carrier of claim 1 wherein the one-time pad is generated by one of the following: a true random number generator, and a pseudorandom number generator operating on a secret key and the identification number of the data carrier.

8. The data carrier of claim 1 for use with a reader, wherein the reader comprises a generator to generate the one-time pad via one of the following: a look-up table, and a pseudorandom number generator operating on a secret key and the identification number of the data carrier.

9. A data carrier comprising:

a memory storing data and a one-time pad;

an index to synchronize a starting position in the one-time pad;

an identification number uniquely associated with the one-time pad; and

a transmitter to transmit the data to the reader.

10. The data carrier of claim 9 for use with a reader, wherein the reader comprises:

a generator to generate the one-time pad; and

a receiver to receive data from the data carrier.

11. The data carrier of claim 10 wherein the receiver further receives the index from the data carrier to synchronize with the starting position in the one-time pad.

12. The data carrier of claim 10 wherein the data carrier and the reader communicate via one of the following interfaces: capacitive interface, inductive interface, electromagnetic interface, optical interface, electrical interface and contact interface.

13. The data carrier of claim 10 wherein the generator generates the one-time pad by one of the following: a look-up table, and a pseudorandom number generator operating on a secret key and the identification number of the data carrier.

14. The data carrier of claim 9 further comprising a controller to prevent reuse of bits in the one-time pad.

15. The data carrier of claim 9 further comprising a counter to index to a next bit in the one-time pad once a bit has been used.

16. The data carrier of claim 9 wherein the data is stored in a first memory and the one-time pad is stored in a second memory.

17. A method comprising the steps of, at a data carrier:

storing a set of data and a one-time pad, wherein the one-time pad is uniquely associated with an identification number;

synchronizing the one-time pad and an index value with an external device to establish a starting position in the one time pad;

requesting from the external device a number of bits from the one-time pad;

receiving a set of bits and a random skip value from the external device; and

if the set of bits received match the one-time pad, incrementing the index by number of bits requested and the skip value, and encrypting and transmitting at least a portion of the set of data.

18. The method of claim 17 wherein the external device performs the following steps:

generating the one-time pad based on the identification number; and

receiving the index value to synchronize with the starting position in the one-time pad.

19. The method of claim 18 wherein the step of generating comprises encrypting the identification number with a secret key.

20. A method for the secure communication of data between a data carrier and a reader comprising:

associating an identification number with a one time pad;

storing the identification number, one-time pad and data on the data carrier;

setting an index, wherein the index identifies a next available bit of the one-time pad;

transmitting the identification number, the index and a challenge to the reader, wherein the challenge at least requests transmission of bits of the one-time pad;

generating the one-time pad in the reader based on the identification number;

transmitting bits of one-time pad, based on the index and challenge and a random skip value, from the reader to the data carrier; and

verifying, at the data carrier, that the bits transmitted from the reader correspond to the challenge, and if correct, incrementing the index by number of

bits in the challenge and the skip value, and encrypting and transmitting at least a portion of the data to the reader.

21. A method for generating a one-time pad comprising the steps of:

providing an identification number;

providing a secret key; and

encrypting the identification number with the secret key.